

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant: Junichiro Yamada et al.

Title: PERSONAL IDENTIFICATION  
DEVICE AND METHOD

Appl. No.: 09/524,693

Filing Date: 3/14/2000

Examiner: Unassigned

Art Unit: Unassigned



**CLAIM FOR CONVENTION PRIORITY**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japan Patent Application No. 11-073561 filed 3/18/1999.

Respectfully submitted,

**JUN 6 2000**

Date \_\_\_\_\_

By \_\_\_\_\_

FOLEY & LARDNER  
Washington Harbour  
3000 K Street, N.W., Suite 500  
Washington, D.C. 20007-5109  
Telephone: (202) 672-5485  
Facsimile: (202) 672-5399

William T. Ellis  
Attorney for Applicant  
Registration No. 26,874

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

1999年 3月18日

出 願 番 号  
Application Number:

平成11年特許願第073561号

出 願 人  
Applicant (s):

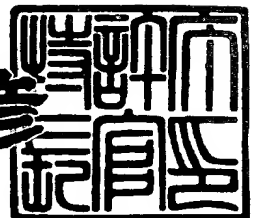
オムロン株式会社



2000年 3月31日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3021479

【書類名】 特許願

【整理番号】 OM58281

【提出日】 平成11年 3月18日

【あて先】 特許庁長官殿

【国際特許分類】 G06T 7/00

【発明者】

【住所又は居所】 京都府京都市右京区花園土堂町 1 0 番地 オムロン株式会社内

【氏名】 山田 純一郎

【発明者】

【住所又は居所】 京都府京都市右京区花園土堂町 1 0 番地 オムロン株式会社内

【氏名】 西川 義治

【特許出願人】

【識別番号】 000002945

【氏名又は名称】 オムロン株式会社

【代表者】 立石 義雄

【代理人】

【識別番号】 100069431

【弁理士】

【氏名又は名称】 和田 成則

【電話番号】 03(3295)1480

【手数料の表示】

【予納台帳番号】 014270

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

特平 11-073561

【包括委任状番号】 9800578

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人認証方法および装置

【特許請求の範囲】

【請求項 1】 ユーザの生体的特徴を検出し、該検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う個人認証方法において、

上記個人認証を行うための少なくとも 1 つの生体的特徴を特定する認証条件データをユーザが携帯する携帯記憶媒体に記憶し、

上記携帯記憶媒体から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行う

ことを特徴とする個人認証方法。

【請求項 2】 上記携帯記憶媒体に、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、

上記ユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行う

ことを特徴とする請求項 1 記載の個人認証方法。

【請求項 3】 上記携帯記憶媒体に、上記生体的特徴データを記憶し、

上記ユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行う

ことを特徴とする請求項 1 記載の個人認証方法。

【請求項 4】 ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、

上記個人認証を行うための少なくとも 1 つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、

上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、

上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段と、

を具備することを特徴とする個人認証装置。

【請求項 5】 上記携帯記憶媒体は、

上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行う

ことを特徴とする請求項 4 記載の個人認証装置。

【請求項 6】 上記携帯記憶媒体は、

上記生体的特徴データを記憶し、

上記認証条件データ読取手段は、

上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行う

ことを特徴とする請求項 4 記載の個人認証装置。

【請求項 7】 ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、

センタ装置と、

上記センタ装置に接続された複数の個人認証端末と、

を具備し、

上記個人認証端末は、

上記個人認証を行うための少なくとも 1 つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、

上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、

上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的

特徴データと照合することでユーザの個人認証を行う認証手段と、

上記センタ装置と通信を行う通信手段と、

を具備することを特徴とする個人認証装置。

【請求項 8】 上記携帯記憶媒体は、

上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行う

ことを特徴とする請求項 7 記載の個人認証装置。

【請求項 9】 上記携帯記憶媒体は、

上記生体的特徴データを記憶し、

上記認証条件データ読取手段は、

上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行う

ことを特徴とする請求項 7 記載の個人認証装置。

【請求項 10】 上記センタ装置は、

各ユーザの上記生体的特徴データを記憶管理し、上記個人認証端末との間の通信により該記憶管理する各ユーザの上記生体的特徴データの更新処理を実行するとともに、上記個人認証端末によるユーザの認識結果を統括制御する

ことを特徴とする請求項 7 記載の個人認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ユーザの指紋、声紋、顔面等の生体的特徴を用いて個人認証を行う個人認証方法および装置に関し、詳しくは、ユーザが携帯する IC カード等の

携帯記憶媒体に記憶された認証条件データに基づき個人認証に使用する生体的特徴を特定して個人認証を行うようにした個人認証方法および装置に関する。

【0 0 0 2】

【従来の技術】

最近、カーナビゲーション、ノートパーソナルコンピュータ、電子手帳、各種モバイル機器等においては指紋、声紋、顔面等の生体的特徴を用いて個人認証を行う個人認証装置が採用されている。

【0 0 0 3】

この指紋認証装置は、ユーザの特定の指の指紋データ、声紋データ、顔面の画像データ等の複数の生体的特徴を示すデータ（以下、これをバイオデータという）を予め登録しておき、装置の起動時等に際しては、この予め登録しておいたバイオデータと使用者から取得したバイオデータとを照合することで個人認証を行い、これにより他人による不正使用等を防止するようにしたものである。

【0 0 0 4】

【発明が解決しようとする課題】

しかし、上記従来の個人認証装置は、いずれもユーザの1つの生体的特徴に着目して構成されたもので、例えば、指紋を用いたものであれば指紋認証端末として構成され、声紋を用いたものであれば、声紋認証端末として構成され、顔面を用いたものであれば画像認証端末として構成されている。

【0 0 0 5】

ところが、ユーザの1つの特定の生体的特徴に着目して構成された個人認証装置においては、障害者や怪我人には使用できない場合もあり、また、正確な個人認証を行うことができない場合がある。

【0 0 0 6】

そこで、ユーザの複数の生体的特徴に着目して個人認証を行う構成も提案されているが、この場合は、指紋認証端末と声紋認証端末との組み合わせ、声紋認証端末と画像認証端末との組み合わせのように複数の認証端末を用いるものであり、いずれの場合も個人認証に用いることができる生体的特徴が固定されているので、自由度に乏しく、また、装置も大型化するという問題があった。



【 0 0 0 7 】

そこで、この発明は、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能であり、かつ高いセキュリティを実現できる個人認証方法および装置を提供することを目的とする。

【 0 0 0 8 】

【課題を解決するための手段】

上記目的を達成するため、請求項 1 記載の発明によれば、ユーザの生体的特徴を検出し、該検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う個人認証方法であって、上記個人認証を行うための少なくとも 1 つの生体的特徴を特定する認証条件データをユーザが携帯する携帯記憶媒体に記憶し、上記携帯記憶媒体から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行う。

【 0 0 0 9 】

このような構成によると、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になる。

【 0 0 1 0 】

また、請求項 2 記載の発明によれば、請求項 1 記載の発明において、上記携帯記憶媒体に、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うことを特徴とする。

【 0 0 1 1 】

このような構成によると、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる。

【 0 0 1 2 】

また、請求項 3 記載の発明によれば、請求項 1 記載の発明において、上記携帯記憶媒体に、上記生体的特徴データを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うことを特徴とする。

【 0 0 1 3 】

このような構成によると、装置本体には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

【 0 0 1 4 】

また、請求項 4 記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、

1) 上記個人認証を行うための少なくとも 1 つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段

2) 上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段

3) 上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段

を具備して構成される。

【 0 0 1 5 】

このような構成によると、ユーザの要望に合わせた複数の生体的特徴を用いる個人認証が可能になる。

【 0 0 1 6 】

また、請求項 5 記載の発明によれば、請求項 4 記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うことを特徴とする。

【 0 0 1 7 】

このような構成によると、ある生体的特徴データに関して装置本体に認証アルゴリズムを持たない場合にも個人認証が可能になる。

【 0 0 1 8 】

また、請求項 6 記載の発明によれば、請求項 4 記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、

上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うことを特徴とする。

## 【0019】

このような構成によると、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

## 【0020】

また、請求項7記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、センタ装置と、上記センタ装置に接続された複数の個人認証端末と、を具備し、上記個人認証端末は、上記個人認証を行うための少なくとも1つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段と、上記センタ装置と通信を行う通信手段と、を具備して構成される。

## 【0021】

このような構成によると、ユーザの要望に合わせた複数の生体的特徴を用いる個人認証が可能になるとともに、この個人認証を集中管理することが可能になる。

## 【0022】

また、請求項8記載の発明によれば、請求項7記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うことを特徴とする。

【 0 0 2 3 】

このような構成によれば、請求項 7 の発明の効果に加えて、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になるという効果を奏する。

【 0 0 2 4 】

また、請求項 9 記載の発明によれば、請求項 7 記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うことを特徴とする。

【 0 0 2 5 】

このような構成によれば、請求項 7 の発明の効果に加えて、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

【 0 0 2 6 】

また、請求項 1 0 記載の発明によれば、請求項 7 記載の発明において、上記センタ装置は、各ユーザの上記生体的特徴データを記憶管理し、上記個人認証端末との間の通信により該記憶管理する各ユーザの上記生体的特徴データの更新処理を実行するとともに、上記個人認証端末によるユーザの認識結果を統括制御することを特徴とする。

【 0 0 2 7 】

このような構成によれば、請求項 7 の発明の効果に加えて、個人認証に用いる生体的特徴データの集中管理も可能になる。

【 0 0 2 8 】

【発明の実施の形態】

以下、この発明に係わる個人認証方法および装置の実施の形態を添付図面を参照して詳細に説明する。

【 0 0 2 9 】

図1は、この発明に係わる個人認証装置の一実施の形態を示す斜視図である。

【0030】

図1において、この個人認証装置100は、ユーザの特定の指の指紋データ、声紋データ、顔面の画像データ等の複数の生体的特徴を示すデータ（バイオデータという）を用いて個人認証を行うもので、ユーザの特定の指の指紋データを採取するためのCCDセンサ20、ユーザの声紋データを採取するためのマイクロフォン30、ユーザの顔面の画像データを採取するためのビデオカメラ40が設けられている。

【0031】

また、各種情報の表示機能および各種情報の入力を行う表示入力パネル部10およびユーザが携帯可能な記憶媒体であるICカード200を挿入可能な挿入口50が設けられている。

【0032】

この実施の形態の個人認証装置100は、個人認証を行うための少なくとも1つの生体的特徴を特定する認証条件データをユーザが携帯するICカード200に記憶し、このICカード200から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行うように構成される。

【0033】

ここで、認証条件データとは、個人認証を行うために使用する生体的特徴（以下、バイオという）を特定するデータで、この実施の形態の個人認証装置100においては、この認証条件データをICカード200から読み取り、この認証条件データに基づきユーザの個人認証を行うバイオを決定する。

【0034】

具体的には、この実施の形態の個人認証装置100においては、個人認証に使用可能なバイオとして

- 1) ユーザの特定の指の指紋
- 2) 声紋
- 3) 顔面の画像
- 4) サイン

の 4 種類が設定されており、認証条件データはこれら 4 種類のバイオのうちの 1 つまたは複数の選択を示すデータである。

【 0 0 3 5 】

図 2 は、図 1 に示した個人認証装置の詳細構成を示すブロック図である。

【 0 0 3 6 】

図 2 において、この個人認証装置 1 0 0 は、表示入力パネル部 1 0、CCD センサ 2 0、マイクロフォン 3 0、ビデオカメラ 4 0、周辺制御部 6 0、IC カードライタリーダー (IC カード R/W) 7 0、メモリ 8 0、中央演算処理部 (CPU) 9 0 を具備して構成される。また、周辺制御部 6 0 は、有線または無線の回線 3 0 1 を介してセンタ装置 3 0 0 に通信可能に接続されている。

【 0 0 3 7 】

ここで、表示入力パネル部 1 0 は、液晶表示装置 (LCD) 1 0 - 1 およびタッチパネル 1 0 - 2 を具備して構成され、液晶表示装置 (LCD) 1 0 - 1 上にタッチパネル 1 0 - 2 を載置した構成をとることにより、各種情報の表示機能および各種情報の入力機能を実現している。

【 0 0 3 8 】

CCD カメラ 2 0 は、周辺制御部 6 0 に接続され、この周辺制御部 6 0 の制御のもとにこの個人認証装置 1 0 0 の使用可能なバイオの 1 つであるユーザの特定の指の指紋に基づき指紋データを読み取るものである。

【 0 0 3 9 】

また、マイクロフォン 3 0 は、周辺制御部 6 0 に接続され、この周辺制御部 6 0 の制御のもとにこの個人認証装置 1 0 0 の使用可能なバイオの他の 1 つであるユーザの声紋に対応する声紋データを取り込むものである。

【 0 0 4 0 】

また、ビデオカメラ 4 0 は、周辺制御部 6 0 に接続され、この周辺制御部 6 0 の制御のもとにこの個人認証装置 1 0 0 の使用可能なバイオの更に他の 1 つであるユーザの顔面に対応する画像データを取り込むものである。

【 0 0 4 1 】

周辺制御部 6 0 は、CCD カメラ 2 0 およびマイクロフォン 3 0 およびビデオ

カメラ 4 0 に接続されるとともに I C カード R / W 7 0 および C P U 9 0 および表示入力パネル部 1 0 に接続され、C C D カメラ 2 0 およびマイクロフォン 3 0 およびビデオカメラ 4 0 による指紋データおよび声紋データおよび顔面の画像データの取り込みを制御するとともに、I C カード R / W 7 0 による I C カード 2 0 0 からのデータの読み出し書き込み動作および表示入力パネル部 1 0 による情報表示入力動作を制御する。

【 0 0 4 2 】

また、周辺制御部 6 0 は、回線 3 0 1 を介してセンタ装置 3 0 0 に接続されており、センタ装置 3 0 0 との通信に基づき各種データの送受を行う。

【 0 0 4 3 】

ここで、センタ装置 3 0 0 は、各ユーザのバイオデータを記憶管理し、個人認証装置 1 0 0 との間の通信によりこの記憶管理する各ユーザのバイオデータの更新処理を実行するとともに、個人認証装置 1 0 0 によるユーザの認識結果を統括制御する。

【 0 0 4 4 】

メモリ 8 0 は、C P U 9 0 を動作させるための制御プログラムとともにこの個人認証装置 1 0 0 の制御に必要な各種情報を記憶している。

【 0 0 4 5 】

O P U 9 0 は、周辺制御部 6 0 に接続されるとともに、メモリ 8 0 に接続されており、メモリ 8 0 に記憶された情報に基づき、周辺制御部 6 0 を介して、この個人認証装置 1 0 0 の各部の動作を統括制御する。

【 0 0 4 6 】

図 3 は、図 1 および図 2 に示した I C カードに記憶されている情報の一例を示す図である。

【 0 0 4 7 】

図 3 に示す構成において、図 1 および図 2 に示した I C カード 2 0 0 には、バイオ実行条件テーブル 2 0 1、指紋バイオ実装テーブル 2 0 2、声紋バイオ実装テーブル 2 0 3、顔面バイオ実装テーブル 2 0 4、指紋本人データ 2 0 5、声紋本人データ 2 0 6、顔面本人データ 2 0 7 等が格納されている。

【0048】

ここで、バイオ実行条件テーブル201は、上述した認証条件データを記憶するテーブルである。

【0049】

また、指紋バイオ実装テーブル202および声紋バイオ実装テーブル203および顔面バイオ実装テーブル204は、それぞれ指紋本人データ205および声紋本人データ206および顔面本人データ207の実装、非実装を示すデータが格納される。

【0050】

ここで、このデータは、「1」または「0」の2値からなり、「1」は対応するバイオデータの実装を示し、「0」は対応するバイオデータの非実装を示す。

【0051】

また、指紋本人データ205は、ユーザ本人から予め取得して登録したユーザの特定の指の指紋に対応する指紋データであり、声紋本人データ206は、ユーザ本人から予め取得して登録したユーザの声紋に対応する声紋データであり、顔面本人データ207は、ユーザ本人から予め取得して登録したユーザの画面に対応する画像データである。

【0052】

図4は、図1および図2に示したICカードに記憶されている情報の他の例を示す図である。

【0053】

図4においては、図3に示した構成に加えて、指紋認証アルゴリズム205-1、声紋認証アルゴリズム206-1、顔面認証アルゴリズム207-1が格納されている。

【0054】

すなわち、図4に示す構成においては、図1および図2に示したICカード200には、バイオ実行条件テーブル201、指紋バイオ実装テーブル202-1、声紋バイオ実装テーブル203-1、顔面バイオ実装テーブル204-1、指紋認証アルゴリズム205-1、指紋本人データ205、声紋認証アルゴリズム



206-1、声紋本人データ206、顔面認証アルゴリズム207-1、顔面本人データ207等が格納されている。

【0055】

ここで、バイオ実行条件テーブル201は、上述した認証条件データを記憶するテーブルである。

【0056】

また、指紋バイオ実装テーブル202-1および声紋バイオ実装テーブル203-1および顔面バイオ実装テーブル204-1は、それぞれ指紋本人データ205および声紋本人データ206および顔面本人データ207の実装、非実装および認証処理をICカード200内部で行うか否かを示すデータが格納される。

【0057】

ここで、このデータは、「1」、「0」、「-1」の3値からなり、「1」は対応するバイオデータの実装を示し、「0」は対応するバイオデータの非実装を示す。また、「-1」は、対応するバイオを用いた認証処理をICカード200内部で行うことを示す。

【0058】

また、指紋認証アルゴリズム205-1、声紋認証アルゴリズム206-1、顔面認証アルゴリズム207-1は、指紋データ、声紋データ、顔面に対応する画像データをを用いた指紋認証アルゴリズム、声紋認証アルゴリズム、顔面認証アルゴリズムを示す。

【0059】

また、指紋本人データ205は、ユーザ本人から予め取得して登録したユーザの特定の指の指紋に対応する指紋データであり、声紋本人データ206は、ユーザ本人から予め取得して登録したユーザの声紋に対応する声紋データであり、顔面本人データ207は、ユーザ本人から予め取得して登録したユーザの画面に対応する画像データである。

【0060】

すなわち、図4に示した構成においては、ICカード200内部に指紋認証、声紋認証、顔面認証を行うアルゴリズムをそれぞれ内蔵しており、これにより、

ＩＣカード２００内部において、指紋認証、声紋認証、顔面認証を行うことができるように構成されている。

【００６１】

図５は、図１および図２に示した個人認証装置における個人認証動作を示すフローチャートである。

【００６２】

なお、図５に示すフローチャートは、ＩＣカード２００内に記憶されるデータが図４に示す構成をとる場合の個人認証装置１００の処理を示している。

【００６３】

図５において、この処理が開始されると、まず、この個人認証装置１００の挿入口５０にユーザの形態するＩＣカード２００が挿入されたかを調べる（ステップ１０１）。ここで、ＩＣカード２００が挿入されていないと判断されると（ステップ１０１でＮＯ）、ステップ１０１に戻り、この個人認証装置１００の挿入口５０にユーザの形態するＩＣカード２００が挿入されるのを待つ。

【００６４】

ステップ１０１で、この個人認証装置１００の挿入口５０にユーザの形態するＩＣカード２００が挿入されたと判断されると（ステップ１０１でＹＥＳ）、ＩＣカードＲ／Ｗ７０によりＩＣカード２００内のデータの読み込みが行われる（ステップ１０２）。

【００６５】

そして、ＩＣカード２００内から読み取ったデータのうちのバイオ実行条件テーブル２０１の内容に基づき表示入力パネル部１０を用いて個人認証に使用するバイオの案内表示を行う（ステップ１０３）。

【００６６】

次に、ユーザの特定の指の指紋データを採取するためのＣＣＤセンサ２０、ユーザの声紋データを採取するためのマイクロフォン３０、ユーザの顔面の画像データを採取するためのビデオカメラ４０を駆動してユーザからバイオ認証データを取得する（ステップ１０４）。

【００６７】

そして、ICカード200内から読み取ったデータのうちの指紋バイオ実装テーブル202-1および声紋バイオ実装テーブル203-1および顔面バイオ実装テーブル204-1を参照して、バイオ実装テーブルは内部指定か、すなわち、バイオの認証をICカード200内で行うか否かの判定を行う（ステップ105）。

## 【0068】

例えば、指紋バイオ実装テーブル202-1の内容が、「1」の場合は、指紋バイオデータの実装を示し、「0」の場合は、指紋バイオデータの非実装を示し、「-1」の場合は、指紋バイオを用いた認証処理をICカード200内部で行うことを示す。

## 【0069】

同様に、声紋バイオ実装テーブル203-1の内容が、「1」の場合は、声紋バイオデータの実装を示し、「0」の場合は、声紋バイオデータの非実装を示し、「-1」の場合は、声紋バイオを用いた認証処理をICカード200内部で行うことを示し、顔面バイオ実装テーブル204-1の内容が、「1」の場合は、顔面バイオデータの実装を示し、「0」の場合は、顔面バイオデータの非実装を示し、「-1」の場合は、顔面バイオを用いた認証処理をICカード200内部で行うことを示す。

## 【0070】

ここで、バイオ実装テーブルは内部指定でない、すなわち、バイオの認証をICカード200内では行わないと判断された場合は（ステップ105でNO）、端末側、すなわち個人認証装置100側の認証アルゴリズムを駆動して認証動作を行う（ステップ106）。

## 【0071】

また、ステップ105で、バイオ実装テーブルは内部指定である、すなわち、バイオの認証をICカード200内で行うと判断された場合は（ステップ105でYES）、ICカード200へユーザから取得したバイオ認証データを転送し（ステップ109）、ICカード200側の認証アルゴリズムを駆動して認証動作を行い（ステップ110）、その認証結果を端末、すなわち、個人認証装置1

00に通知する（ステップ111）。

【0072】

次に、バイオ実装テーブルで複数の指定終了か、すなわち、指定した全てのバイオを用いた認証動作が終了かを調べる（ステップ107）。ここで、バイオ実装テーブルで複数の指定終了でない、すなわち、指定した全てのバイオを用いた認証動作が終了していないと判断された場合は（ステップ107でNO）、ステップ103に戻り、ステップ103からステップ107の処理を繰り返す。

【0073】

そして、ステップ107で、バイオ実装テーブルで複数の指定終了、すなわち、指定した全てのバイオを用いた認証動作が終了したと判断されると（ステップ107でYES）、その認証結果を出力して表示入力パネル部10に表示し（ステップ108）、この処理を終了する。

【0074】

なお、上記説明においてはICカード200内に記憶されるデータが図4に示す構成をとる場合の個人認証装置100の処理を示したが、ICカード200内に記憶されるデータが図3に示す構成をとる場合は、全ての認証処理が個人認証装置100側で行われることになり、図5に示した処理のうちのステップ105の処理およびステップ109から111の処理が省略される。

【0075】

【発明の効果】

以上説明したように、請求項1記載の発明によれば、ユーザの生体的特徴を検出し、該検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う個人認証方法であって、上記個人認証を行うための少なくとも1つの生体的特徴を特定する認証条件データをユーザが携帯する携帯記憶媒体に記憶し、上記携帯記憶媒体から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行うように構成したので、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になるとともに高いセキュリティが実現できる。

【0076】

また、請求項 2 記載の発明によれば、請求項 1 記載の発明において、上記携帯記憶媒体に、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うように構成したので、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる。

## 【 0 0 7 7 】

また、請求項 3 記載の発明によれば、請求項 1 記載の発明において、上記携帯記憶媒体に、上記生体的特徴データを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うように構成したので、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

## 【 0 0 7 8 】

また、請求項 4 記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、上記個人認証を行うための少なくとも 1 つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段とを具備して構成したので、ユーザの要望に合わせた複数の生体的特徴を用いる個人認証が可能になるとともに高いセキュリティが実現できる個人認証装置を提供することができる。

## 【 0 0 7 9 】

また、請求項 5 記載の発明によれば、請求項 4 記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個

人認証を行うように構成したので、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる個人認証装置を提供することができる。

## 【0080】

また、請求項6記載の発明によれば、請求項4記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うように構成したので、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる個人認証装置を提供することができる。

## 【0081】

また、請求項7記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、センタ装置と、上記センタ装置に接続された複数の個人認証端末と、を具備し、上記個人認証端末は、上記個人認証を行うための少なくとも1つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段と、上記センタ装置と通信を行う通信手段と、を具備して構成したので、ユーザの要望に合わせた複数の生体的特徴を用いる個人認証が可能になるとともに、この個人認証を集中管理することが可能になる個人認証装置を提供することができる。

## 【0082】

また、請求項8記載の発明によれば、請求項7記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の

認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うように構成したので、請求項 7 の発明の効果に加えて、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる個人認証装置を提供することができる。

## 【 0 0 8 3 】

また、請求項 9 記載の発明によれば、請求項 7 記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うように構成したので、請求項 7 の発明の効果に加えて、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる個人認証装置を提供することができる。

## 【 0 0 8 4 】

また、請求項 1 0 記載の発明によれば、請求項 7 記載の発明において、上記センタ装置は、各ユーザの上記生体的特徴データを記憶管理し、上記個人認証端末との間の通信により該記憶管理する各ユーザの上記生体的特徴データの更新処理を実行するとともに、上記個人認証端末によるユーザの認識結果を統括制御するように構成したので、請求項 7 の発明の効果に加えて、個人認証に用いる生体的特徴データのを集中管理が可能になる個人認証装置を提供することができるという効果を奏する。

## 【図面の簡単な説明】

## 【図 1】

この発明に係わる個人認証装置の一実施の形態を示す斜視図である。

## 【図 2】

図 1 に示した個人認証装置の詳細構成を示すブロック図である。

## 【図 3】

図1および図2に示したICカードに記憶されている情報の一例を示す図である。

【図4】

図1および図2に示したICカードに記憶されている情報の他の例を示す図である。

【図5】

図1および図2に示した個人認証装置における個人認証動作を示すフローチャートである。

【符号の説明】

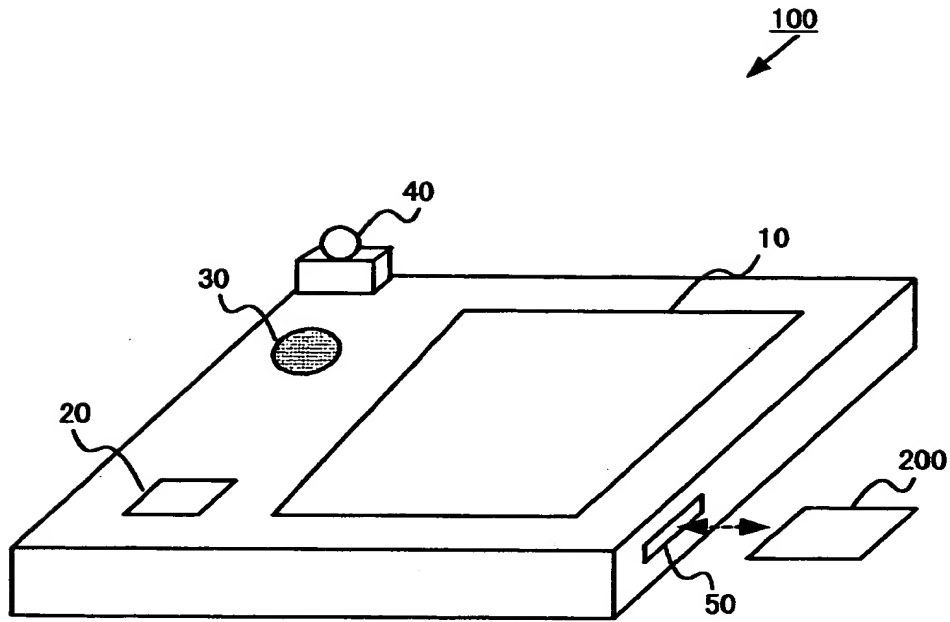
- 10 表示入力パネル部
- 20 CCDセンサ
- 30 マイクロフォン
- 40 ビデオカメラ
- 50 ICカード挿入口
- 60 周辺制御部
- 70 ICカードライタリーダ (ICカードR/W)
- 80 メモリ
- 90 中央演算処理部 (CPU)
- 100 個人認証装置
- 200 ICカード
- 201 バイオ実行条件テーブル
- 202 指紋バイオ実装テーブル
- 202-1 指紋バイオ実装テーブル
- 203 声紋バイオ実装テーブル
- 203-1 声紋バイオ実装テーブル
- 204 顔面バイオ実装テーブル
- 204-1 顔面バイオ実装テーブル
- 205 指紋本人データ
- 205-1 指紋認証アルゴリズム



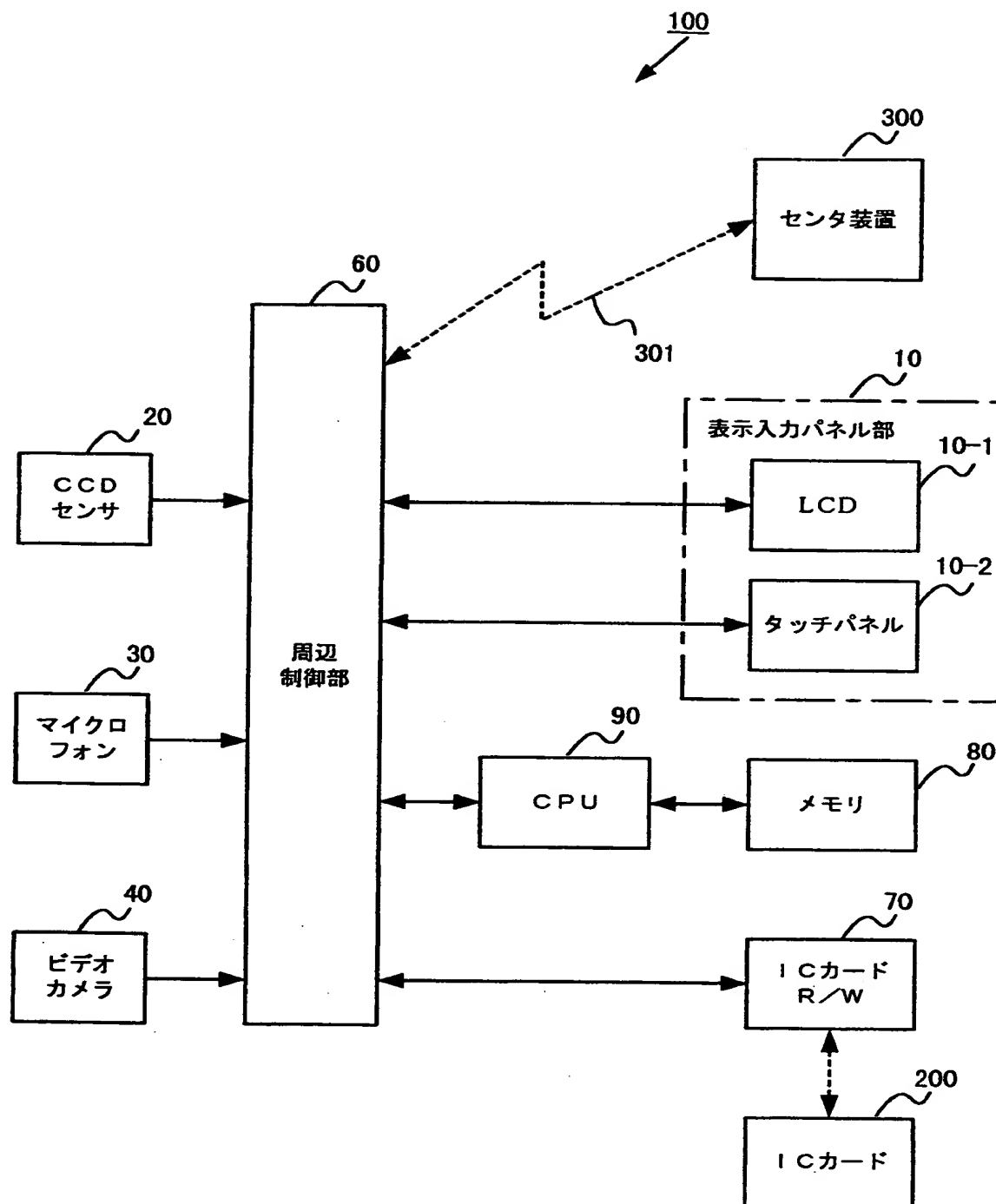
- 206 声紋本人データ
- 206-1 声紋認証アルゴリズム
- 207 顔面本人データ
- 207-1 顔面認証アルゴリズム
- 300 センタ装置
- 301 回線

【書類名】 図面

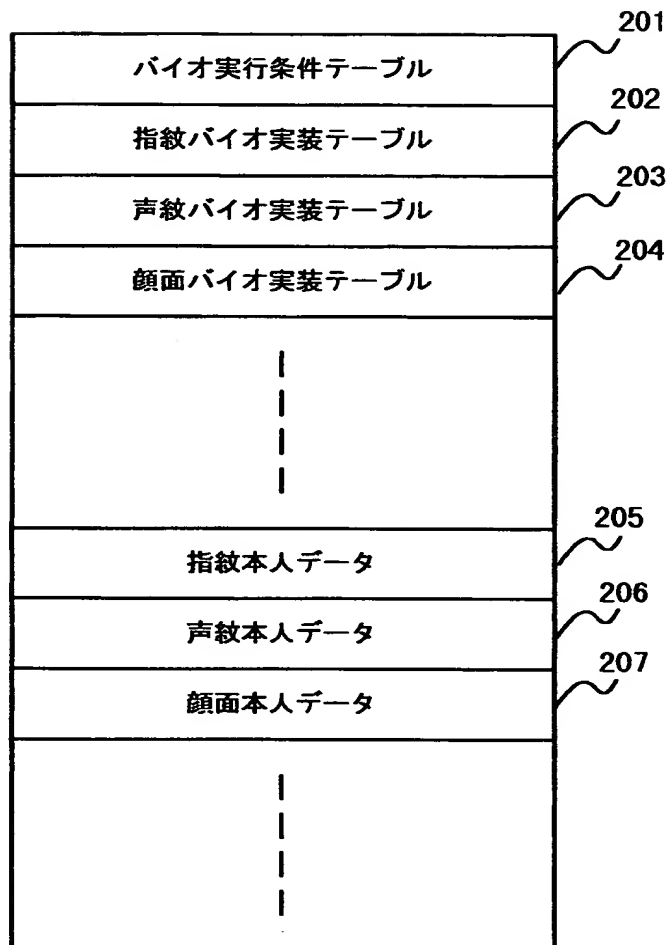
【図 1】



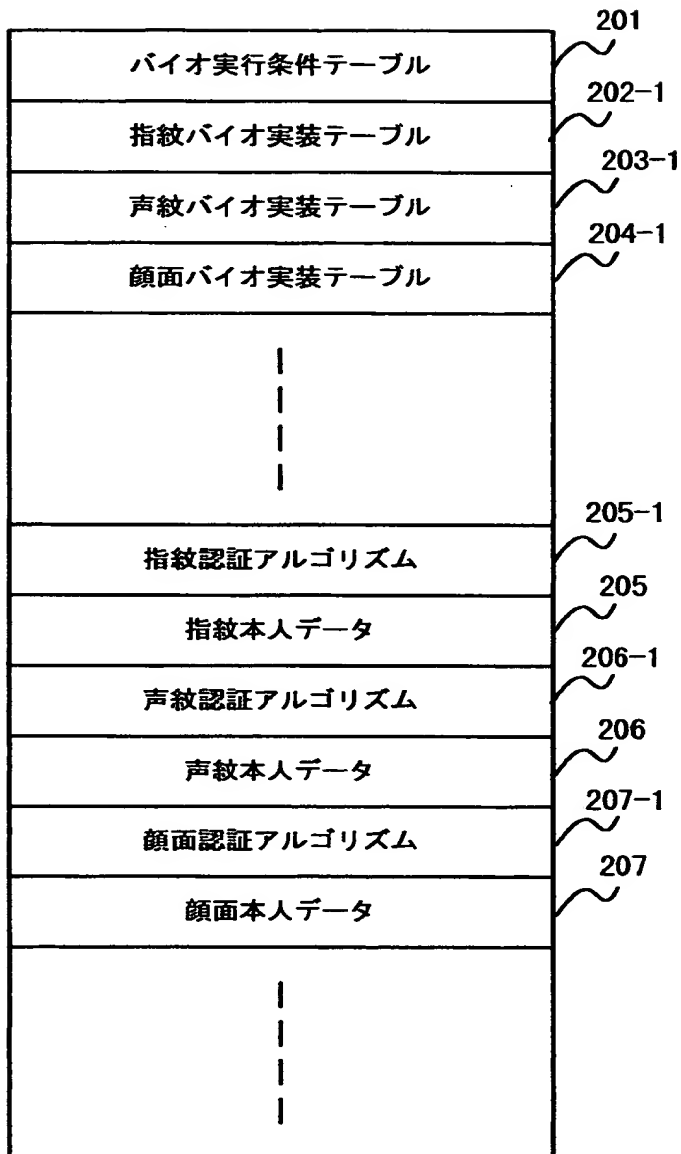
【図 2】



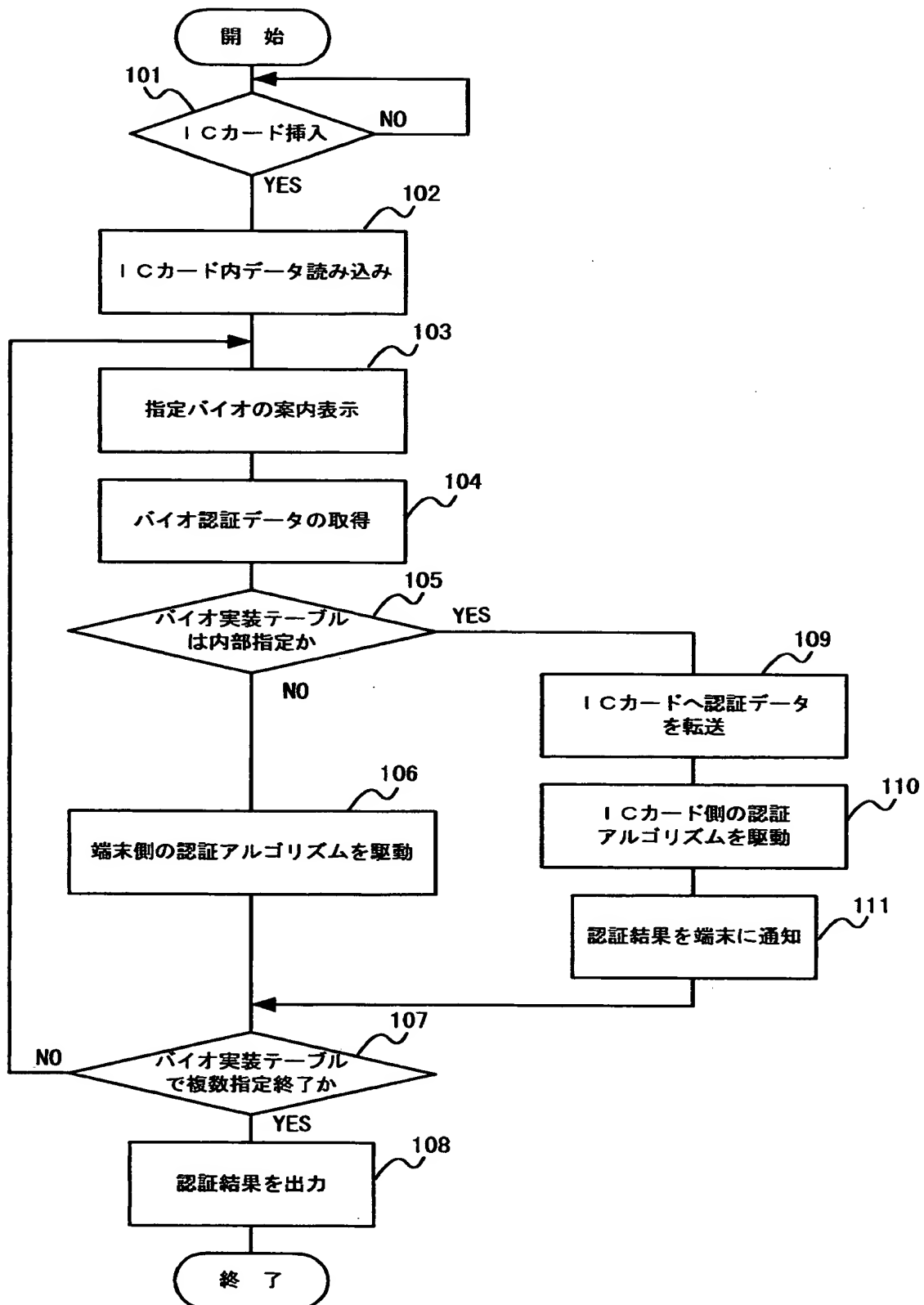
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能であり、かつ高いセキュリティを実現できる個人認証方法および装置を提供する。

【解決手段】 個人認証を行うための少なくとも1つの生体的特徴を特定する認証条件データをユーザが携帯するICカード200に記憶し、このICカード200から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行う。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000002945]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 京都府京都市右京区花園土堂町10番地  
氏 名 オムロン株式会社